Remarks

In the present paper, Claims 1, 3-9, 20, 22-28, 39, 41-47 and 58-72 are pending. The claims have not been amended.

35 U.S.C. § 112, second paragraph

Claims 1, 3-9, 20, 22-28, 39, 41-47, 58-72 stand rejected under 35 U.S.C. § 112, second paragraph. Claims 1, 20 and 39 are in independent form.

The Examiner argues that there is insufficient antecedent basis for the recitation of "network communications" in each of independent claims 1, 20 and 39 because it is unclear how other "types" of communications recited in the claims are associated with network communications. The Examiner further argues that there is insufficient antecedent basis for the recitation of "the selection among the target hosts" because it is unclear what the distinction is between the selected hosts and "selected ones of the plurality of target hosts which are associated with end-to-end secure network communications[1].

The applicants respectfully traverse these rejections. According to the M.P.E.P. §2173.02, a claim element is definite within the meaning of 35 U.S.C. §112, second paragraph, if the claim language provides at least a *reasonable degree* of particularity and distinctness. Some latitude in the manner of expression and the aptness of terms should be permitted even though the claim language is not as precise as the examiner might desire. Moreover, in reviewing a claim for compliance with 35 U.S.C. §112, second paragraph, the Examiner must consider the claim *as a whole* to determine whether the claim apprises one of ordinary skill in the art of its scope[2]. For example, Claim 1 recites:

[1] See Office action mailed 10-27-2006, Pages 2-3
[2] See for example, *Orthokinetics, Inc. v. Safety Travel Chairs, Inc.*, 806 F.2d 1565, 1576, 1 USPQ2d 1081, 1088 (Fed. Cir. 1986).

A method for providing secure communications over a network in a distributed workload environment having target hosts which are accessed through a distribution processor by a common network address, the method comprising the steps of:

routing both inbound and outbound communications with target hosts which are associated with an end-to-end secure network communication through the distribution processor;

processing both inbound and outbound end-to-end secure network communications at the distribution processor so as to provide endpoint network security processing of communications from the target host and endpoint network security processing of communications to the target host;

receiving at the distribution processor, network communications directed to the common network address;

encapsulating communications between the distribution processor and selected ones of the plurality of target hosts which are associated with end-to-end secure network communications; and

distributing the received network communications that are directed to the common network address among selected ones of the target hosts, wherein the selection among the target hosts is carried out so as to distribute workload associated with the network communications among the target hosts.

Thus, in a distributed workload environment, target hosts are accessed through a common network address by a distribution processor. Network communications that are directed to the common network address are *received* at the distribution processor, and the distribution processor distributes the received (inbound) network communications that are directed to the common network address among *selected ones of the target hosts* so as to distribute the workload associated with the network communications among the target hosts.

By way of illustration, and not by way of limitation, Fig. 4 of the present application is reproduced herein to demonstrate an exemplary arrangement where a client 10 communication across the network 12 (a network communication directed to a common network address) is received at the distribution processor 50. As an example, assume that a first network communication is *not* a secure end-to-end network communication. The distribution processor 50 may select to distribute the first network communication to server 56 so as to distribute the workload associated with the network communications among the target hosts.

For the first network communication, there is no need to route the response from server 56 through the distribution processor 50 to the client 10, unless for example, outbound router load balancing or other like operations are being performed. As such, server 56 may provide an outbound network communication back to the client, as illustrated in the figure by the arrow from server 56 back to network 12.

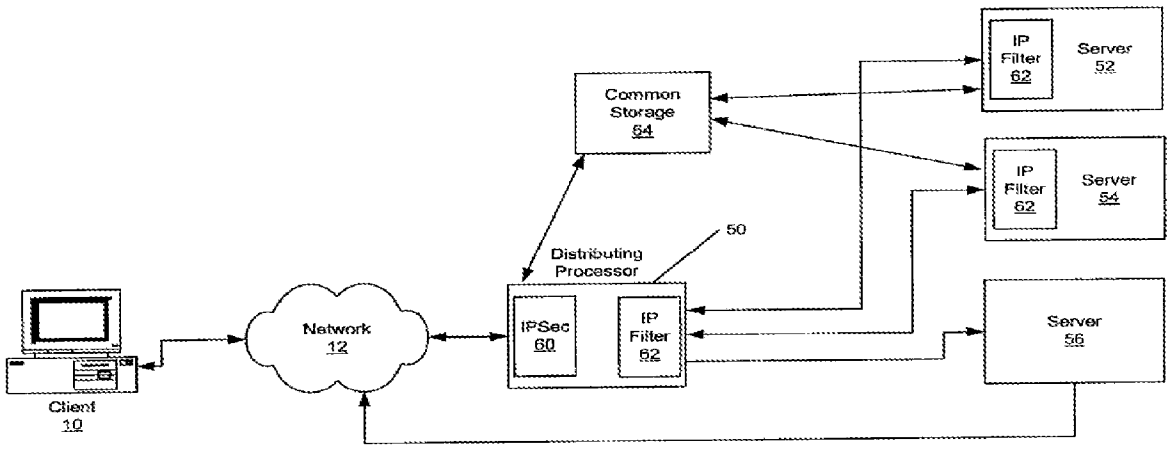

Figure 4

However, as an example, certain virtual private network (VPN) technologies, such as IPSEC, implement network communications as end-to-end secure network communications. As noted in the applicants' specification, certain workload distribution methods experience compatibility problems with IPSEC[3]. Compatibility issues with end-to-end security, such as IPSEC, in certain workload distribution methods are also recognized in the art cited by the Examiner in the current Office action[4] and are also described in greater detail herein.

Accordingly, claim 1 further recites routing both inbound and outbound communications with target hosts which are associated with an end-to-end secure network

[3] See the applicant's published patent application U.S. Pat. Pub. No. US2002/0095603, paragraph 0022-32.
[4] See U.S. Pat. No. 6,266,335 to *Bhaskaran,* Col. 2, lines 43-58.

communication through the distribution processor and processing both inbound and outbound end-to-end secure network communications at the distribution processor so as to provide endpoint network security processing of communications from the target host and endpoint network security processing of communications to the target host.

Again, with reference to Fig. 4 herein, a network communication may comprise an end-to-end network communication, such as where a given network communication utilizes an IP security technology such as IPSEC. If a network communication is an end-to-end secure network communication, then the distribution processor processes the (inbound and outbound) end-to-end secure network communications. That is, for purposes of satisfying the network security requirements of the particular end-to-end secure network communication protocol utilized, the distribution processor may serve and an endpoint and provide endpoint network security processing (e.g., the client being the other endpoint).

However, the transaction with the client must still be satisfied. As such, inbound and outbound communications that are associated with the end-to-end network secure communication may be routed between the distribution processor and a selected target host.

As yet a further illustrative example, assume that client 10 sends a second network communication, which is an end-to-end secure network communication directed to the common network address that is received by the distribution processor 50. The distribution processor 50 selects one of the target hosts to receive the distributed communication. Assume that target host 54 is selected this time. Because the exemplary second communication is an end-to-end secure network communication, the distribution processor may provide endpoint network security processing of communications from the target host (to the client), e.g., to satisfy the requirements of the corresponding security protocol. Moreover, because the distribution processor may provide endpoint network security processing, inbound and outbound communications with the target host (target host 54 in the example) are routed through the distribution processor. Thus, the target host 54 sends its outbound communication through the distribution processor 50. The

distribution processor sends the outbound network communication (via network 12) back to the client 10 and satisfies the end-to-end security requirements.

Moreover, communications between the distribution processor 50 and the selected one of the plurality of target hosts which are associated with end-to-end secure network communications, target host 54 in this example, are encapsulated. For example, encapsulation, among other things, may enable consistent policies to be provided that bypass IP filtering for such encapsulated communications. Normal IP filtering may then be applied to other communications. Accordingly, existing IP filtering externals need not be changed and a consistent policy may be provided for all processing systems in the cluster of data processing systems.

In view of the clarifying remarks herein, the applicants believe that, when reading the claim 1 *as a whole*, the claim recitations are definite within the meaning of 35 U.S.C. § 112, second paragraph. Thus, the applicants request that the rejections to claim 1 and the claims that depend there from are withdrawn.

Independent claims 20 and 39 were rejected under 35 U.S.C. § 112, second paragraph based upon reasons similar to those used to reject claim 1. Accordingly, the arguments set out in detail above, apply by analogy to claims 20 and 39. Thus, the applicants request that the rejection to claims 20, 39 and the claims that depend there from are withdrawn.

35 U.S.C. § 102(e)

Claims 1, 7, 20, 26, 39, 45 and 58-72 were rejected under 35 U.S.C. §102(e) as being unpatentable over U.S. Pat. No. 6,266,335 to *Bhaskaran*. According to the M.P.E.P. §706.02, in order to be anticipating under §102, the reference must teach every aspect of the claimed invention[5]. Of the rejected claims, claims 1, 20 and 39 are in independent form.

[5] See also *Carella v. Starlight Archery and Pro Line Co.*, 804 F.2d 135, 138, 231 U.S.P.Q. 644, 646 (Fed. Cir. 1986).

With regard to claim 1, as amended herein, *Bhaskaran* fails to teach or suggest:

> routing both inbound and outbound communications with target hosts which are associated with an end-to-end secure network communication through the distribution processor…processing both inbound and outbound end-to-end secure network communications at the distribution processor so as to provide endpoint network security processing of communications and … encapsulating communications between the distribution processor and selected ones of the plurality of target hosts which are associated with end-to-end secure network communications.

Remaining independent claims 20 and 39 recite similar limitations. As such, the arguments set out below apply by analogy to these claims.

Bhaskaran discloses a flow switch 205 that allows multiple IP servers in a cluster 200 to share the same IP address by performing *Data Link Layer address* translation of packets flowing from an IP client to a selected one of the IP servers in the cluster[6].

However, as will be described in greater detail below, the claimed recitation of a distribution processor does not read on the flow switch 205 or any other component taught or suggested in *Bhaskaran*, regardless of whether the flow switch 205 provides simplex or duplex processing of packets sent to (or from) a common network address. This can be seen because there is no teaching or suggestion in *Bhaskaran* whatsoever, of a distribution device that performs endpoint network security processing of communications from the target host and endpoint network security processing of communications to the target host as claimed.

In fact, *Bhaskaran* explicitly teaches away from that which is claimed. For example, in *Bhaskaran*, each of the servers 210-250 in the cluster 200 share the same virtual IP address, but have a distinct Data Link Layer address[7]. The flow switch 205 uses the Data Link Layer address (Layer 2) to translate the virtual IP address (Layer 3) from inbound clients to a physical address

[6] See for example, *Bhaskaran*, Col. 5, lines 34-37.
[7] See for example, *Bhaskaran*, Col. 5, lines 47-54.

(e.g., based upon the IP server's MAC address) after the IP server is selected by the flow switch[8]. Under this arrangement, the flow switch 205 can pass the packets on to an IP server without the need to modify IP (Layer 3) information. Accordingly, the flow switch 205 can pass packets with encrypted payloads and/or hashed IP headers (such as with IPSEC) to the assigned IP server *without acting as an endpoint*.

The format of a packet 300 transmitted over an external network is illustrated in FIG. 3A of *Bhaskaran* as including a header field 310, a link field 320, an IP header 330, a TCP header 340, a data payload 350, a CRC field 360 and a trailer 370. The IP header 330 and the TCP header 340 are standard IP and TCP headers and the CRC field 360 contains a checksum correction code used to verify that packet 300 has been transmitted without error[9].

As noted in *Bhaskaran*:

> … If IP header 330 were modified… the checksum for CRC field 360 would have to be recalculated, an operation requiring processor intervention. In addition, if encrypted information is transmitted according to the IPSEC security framework, decryption of the IP payload is required. *Thus, by eliminating the need to recompute the checksum for each packet*, the network flow switch of the present invention achieves better throughput than prior art devices. Network owners can further deploy IPSEC security mechanisms transparently and without fear of communications being broken[10]. (emphasis added)

Thus, the flow switch 205 explicitly does not participate in, and explicitly avoids, endpoint network security processing of communications. Rather, the flow switch 205 passes the packets to the selected IP server in the cluster in such a way that decrypting and other endpoint network security processing is not performed at the flow switch. The "fear of communications being broken" is avoided because the selected IP server (and not the flow switch) is apparently treated as the endpoint for both inbound and outbound packets.

[8] See for example, *Bhaskaran*, Col. 5, lines 56-63.
[9] See for example, *Bhaskaran*, Col. 6, lines 27-50.
[10] See for example, *Bhaskaran*, Col. 6, lines 38-50.

This passage from *Bhaskaran* is best understood in view of how the flow switch 205 works and in view of how an end-to-end security technology such as IPSEC works. As best seen in FIG. 3B of *Bhaskaran*, the Link field 320 (shown as part of the packet in Fig. 3A) includes a Data Link Layer source address field 380, a Data Link Layer destination address field 390 and type field 395.

The flow switch 205 routes packets to a select one of the IP servers by writing the MAC address (Layer 2) of the selected server into the Data Link Layer destination address field 390 of each packet 300. This can be seen with reference to Fig. 2 of *Bhaskaran*, which illustrates that each of the servers 210-250 share the same virtual IP address (Layer 3), but have a unique Layer 2 address (their unique MAC address).

This avoids modifications to the IP header or other IP layer information of the packet. For example, the IP header of packets sent using the Authentication Header protocol of IPSEC is hashed. As such, changes to the IP header by the flow switch 205 could create broken communications and other interoperability issues with IPSEC.

This also avoids problems with the Encapsulating Security Payload protocol of IPSEC because any change of an IP address implies a change in the CRC checksum. However, the checksum *is included in the encrypted payload*. Notably, *Bhaskaran* explicitly teaches that the CRC checksum is not recomputed[11]. However, since the link field 320 is not part of the IP protocol, there is no need to recalculate the checksum for CRC field 360 when link field 320 is modified.

Further, if the flow switch 205 is used for outbound operations, i.e., from an IP server in the cluster to the IP client, Data Link Layer address translation is not required to be performed by the flow switch[12]. An outbound flow from the IP servers to the routers as taught by *Bhaskaran*

[11] See also, *Bhaskaran*, Col. 2, lines 43-65.
[12] See Bhaskaran, Col. 5, lines 44-47.

is illustrated in Fig. 4C. As is clearly evident in the flow chart of Fig. 4C, the flow switch receives a packet from an IP server, optionally changes a MAC (Layer 2 Data Link Layer) destination address and sends the packet on to an associated router[13]. Thus, if a router goes down, the IP servers do not need to take action because the flow switch can automatically handle redirection. However, this neither teaches nor suggests performing endpoint network security processing. Rather, it teaches *avoiding* endpoint network security processing at a distributor.

Accordingly, *Bhaskaran* does not teach or suggest routing both inbound and outbound communications with target hosts which are associated with an end-to-end secure network communication through the distribution processor…processing both inbound and outbound end-to-end secure network communications at the distribution processor so as to provide endpoint network security processing of communications as claimed.

Still further, merely changing a Layer 2 Destination address field to map a packet directed to a virtual IP address to a specific IP server's MAC address neither teaches nor suggests encapsulating communications between the distribution processor and selected ones of the plurality of target hosts which are associated with end-to-end secure network communications. Encapsulation is not taught or suggested. Moreover, *Bhaskaran* explicitly teaches that even if the flow switch 205 is used in a duplex operation, there is no need to manipulate outbound packets at all. Rather, the flow switch may be used for duplex for example, to address outbound load balancing to the routers, to address issues flow when a router becomes unavailable, etc[14].

Accordingly, *Bhaskaran* does not teach or suggest encapsulating communications between the distribution processor and selected ones of the plurality of target hosts which are associated with end-to-end secure network communications as claimed.

---

[13] See Bhaskaran, Col. 7, line 51 through Col. 8, line 8.
[14] See Bhaskaran, Col. 8, lines 8-65.

In view of the amendments and clarifying comments herein, the Applicants respectfully request that the Examiner withdraw the rejections to claims 1, 20, 39 and the claims that depend therefrom under 35 U.S.C. §102(e).

35 U.S.C. §103

Claims 3-6, 8, 9, 22-25, 27, 28, 41-44, 46 and 47 were rejected under 35 U.S.C. §103(a) as being unpatentable over *Bhaskaran* in view of U.S. Pat. No. 6,826,559 to Shaffer et al. (hereinafter, *Schaffer*).

According to the MPEP §706.02(j), to establish a *prima facie* case of obviousness, the prior art reference must teach or suggest all the claim limitations[15]. It is the applicants' position that a *prima facie* case of obviousness has not been established for the claims set out herein as these claims depend from one of claims 1, 20 or 39, which applicants now believe are patentable over the art of record.

Moreover, cited references, even when combined, fail to teach or suggest all of the limitations of the above-claims as amended herein. For example, *Schaffer* teaches techniques for handling objects in a network cache using a cost function. A cache enabled router reads a packet header and decides whether the packet is a TCP packet. If the packet is a TCP packet and the packet is destined for port 80, the router encapsulates the packet and sends it to a selected cache by adding another TCP header that specifies the selected cache as the destination address[16]. As such, even though a packet is "encapsulated", this is only to direct the packet to a network cache and is not between a distribution processor and a target host.

As such, Schaffer neither teaches nor suggests as claimed:

> routing both inbound and outbound communications with target hosts which are associated with an end-to-end secure network communication through the distribution processor…processing both inbound and outbound end-to-end

[15] See also, *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991); MPEP § 2143 - § 2143.03
[16] See for example, *Shaffer*, Col. 5, line 45 through Col. 6, line 10 and Fig. 3.

> secure network communications at the distribution processor so as to provide endpoint network security processing of communications and … encapsulating communications between the distribution processor and selected ones of the plurality of target hosts which are associated with end-to-end secure network communications.

In view of the amendments and clarifying comments herein, the Applicants respectfully request that the Examiner withdraw the rejections to claims 3-6, 8, 9, 22-25, 27, 28, 41-44, 46 and 47 under 35 U.S.C. §103(a).

Conclusion

For all of the above reasons, the applicants respectfully submit that the above claims recite allowable subject matter. The Examiner is encouraged to contact the undersigned to resolve efficiently any formal matters or to discuss any aspects of the application or of this response. Otherwise, early notification of allowable subject matter is respectfully solicited.

Respectfully submitted,
Stevens & Showalter, L.L.P.
By
/Thomas E. Lees/
Reg. No. 46,867

7019 Corporate Way
Dayton, Ohio 45459-4238
Phone 937-438-6848
tlees@sspatlaw.com